ABSTRACT OF THE DISCLOSURE

A voter V_i encrypts his vote content v_i with a public key k_{PC} of a counter C, then concatenates the encrypted vote content x_i with a tag t_i to obtain a ballot z_i, then randomizes it with a random number r_i to create a preprocessed text e_i, and sends it and a signature s_i therefor to an election administrator A. The administrator A generates a blind signature d_i for the preprocessed text e_i and sends it back to the voter V_i. The voter V_i excludes the influence of the random number r_i from the blind signature d_i to obtain administrator signature y_i, and sends vote data $<z_i, y_i>$ to a counter C. The counter C verifies the validity of the administrator signature y_i and, if valid, generates and publishes a vote list containing the data $<z_i, y_i>$ to the voter V_i. The voter V_i checks the vote list to make sure that it contains the data $<z_i, y_i>$ with his tag t_i held in the ballot z_i. The counter C decrypts the encrypted vote content x_i in the ballot z_i to obtain the vote content v_i, and counts the number of votes polled for each candidate.